

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

FILED
RICHARD W. NAGEL
CLERK OF COURT

2019 MAY -1 PM 3:15

U.S. DISTRICT COURT
SOUTHERN DIST OHIO
WEST DIV CINCINNATI

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH 5
EMAIL ADDRESSES FURTHER
DESCRIBED IN ATTACHMENT A THAT
ARE STORED AT PREMISES
CONTROLLED BY GOOGLE LLC.

Case No. **1:19MJ-326**

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Paul W. Cox, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google LLC, an email provided that is headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC to disclose to the government copies of the information (including the content of communications) associated with the following email accounts --

KLIZOSIROTA@GMAIL.COM (SUBJECT GMAIL ACCOUNT 1)

KLIZOB@GMAIL.COM (SUBJECT GMAIL ACCOUNT 2)

DJCADZOW@GMAIL.COM (SUBJECT GMAIL ACCOUNT 3)

KELLYCOMATOSE@GMAIL.COM (SUBJECT GMAIL ACCOUNT 4)

CRYPTOKLIZO@GMAIL.COM (SUBJECT GMAIL ACCOUNT 5)

Further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent for the Food and Drug Administration-Office of Criminal Investigations ("FDA-OCI"). I am currently assigned to the Kansas City Field Office, and am the Seized Computer Evidence Recovery Specialist/Computer Forensics Agent for the Kansas City Region. My current duties include investigating violations of the Federal Food Drug and Cosmetic Act and other violations of the United States Criminal Code. I have been employed as a Special Agent since November 2012. Prior to my current position with FDA-OCI, I was employed as a Special Agent with the Department of Health and Human Service ("HHS") Office of Inspector General Computer Crimes Unit, stationed at the Centers for Disease Control and Prevention and the HHS Computer Security Incident Response Center, and prior to that I was a Special Agent with the National Aeronautics and Space Administration-Office of Inspector General ("NASA-OIG") Computer Crimes Division, stationed at the Jet Propulsion Laboratory. I am a graduate of the following training programs: Criminal Investigator Training Program and the Seized Computer Evidence Recovery Specialist Program at the Federal Law Enforcement Training Center (2013), Inspector General Criminal Investigator Academy (2014), HHS Special Agent Basic Training Program (2016), and the FDA-OCI Special Agent Training Program (2018). During my career, I have received specialized training in the investigation of computer crimes, combating the distribution of child pornography, the performance of digital forensics, and investigating the sale of counterfeit, adulterated, and misbranded drugs via the internet and dark web. Additionally, I have presented training to other federal law enforcement officers in the United States on the topic of cyber investigations and have presented training on the investigation of the online sale of counterfeit

drugs to international law enforcement officials at the Interpol Global Complex for Innovation in Singapore. Through the course of my duties, I have conducted numerous investigations into the distribution of counterfeit, misbranded, and adulterated drugs and controlled substances via the dark web and United States Postal Service, and personally executed approximately 30 undercover purchases of drugs via the dark web in exchange for cryptocurrency. Through the course of my duties I have participated in the execution of numerous search warrants.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, United States Code, Sections 841(a)(1), 846, 331(a), 331(k), and 331(i), and Title 18, United States Code, Section 1957 (hereinafter the “**TARGET OFFENSES**”) have been committed by **Khleri Sirotkin**, and others yet unknown. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. FDA-OCI are investigating the distribution of counterfeit and misbranded opiate-based prescription drugs by a seller using the moniker “Pill-Cosby” and “SlangGang” on Darknet Marketplace known as Dream Market, Wall Street, and Empire Market. From a series of undercover

purchases, I have learned that all of the drugs sold by Pill-Cosby and SlangGang are sent through the USPS, using postage paid for using bitcoin cryptocurrency. Furthermore, records of the purchases of items used in the manufacture of counterfeit drugs indicate that Sirotkin has purchased several items consistent with counterfeit drug manufacturing, and that Sirotkin utilizes his mobile phone and email accounts in furtherance of his drug trafficking organization.

7. Over the past year, FDA-OCI, working with the Drug Enforcement Administration, the United States Postal Inspection Service, the Federal Bureau of Investigation, and Homeland Security Investigations have been investigating opiate-based prescription drugs being advertised and sold on Darknet Marketplaces, and distributed through the USPS.

8. From my participation in this investigation, my knowledge, training and experience, my review of investigation reports by other members of the investigative team and discussions with other federal agents involved in the investigation of individuals involved in the distribution of misbranded and counterfeit opiate-based prescription drugs via the USPS, I know the information included in the following paragraphs.

9. In general, an email that is sent to a Google LLC, subscriber is stored in the subscriber's "mail box" on Google LLC servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google LLC, servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google LLC's, servers for a certain period of time.

I. Investigation of "Pill-Cosby" and "SlangGang"

10. Between April 2018 and April 2019, agents from the Food and Drug Administration -- Office of Criminal Investigations (FDA-OCI), the Federal Bureau of Investigations (FBI), the United States Postal Inspection Service (USPIS), Homeland Security Investigations (HSI), and the

Drug Enforcement Administration (DEA) have been conducting an investigation into the manufacture and distribution of counterfeit oxycodone tablets originating from the Las Vegas-area, sold via the darkweb marketplaces Dream Market, Wall Street Market, and Empire Market in exchange for bitcoin cryptocurrency, and distributed via the United States Postal Service.

11. A review of the vendor pages on Dream Market, Wall Street Market, and Empire Market has shown that the vendor Pill-Cosby has been active since September 2017 and is responsible for over 5,800 transactions with an estimated \$2.35M (USD) in sales, and that SlangGang has been active since June 2018 and is responsible for over 1,100 transactions with an estimated \$235,000 (USD) in sales.

12. During the course of this investigation, ten (10) undercover purchases have been made from the monikers SlangGang and Pill-Cosby between April 2018 and April 2019, including purchases delivered to the Southern District of Ohio. In each of these undercover purchases, agents placed an order for counterfeit oxycodone tablets in exchange for Bitcoin cryptocurrency. In each of these instances the drugs were purchased without a valid prescription and they were dispensed in packaging that did not bear proper instructions for use or warnings. In the case of each purchase, an undercover agent placed an order for counterfeit oxycodone pills in exchange for Bitcoin cryptocurrency, and provided an undercover address to which the purchase was to be delivered.

13. In each case, agents subsequently received parcels to the undercover addresses provided at the time of the purchases. These parcels contained items matching the description of the items purchased by the undercover agent. The contents included tablets, of various quantities, blue in color, round in shape, bearing pill imprints "A 215" and a half-tablet score mark. The parcels were all found to bear postage purchased from the USPS reseller EasyPost, and originated from the Las Vegas, Nevada, area.

14. Based on my training and experience, I know that the pill imprint A 215 is associated with a 30 mg oxycodone HCL tablet sold by Actavis. I also know that oxycodone HCL is a Schedule II controlled substance.

15. A review of USPS databases indicates that all of the parcels received following purchases from Pill-Cosby and SlangGang were purchased by an EasyPost postage meter associated with BitcoinPostage.info. Based on my training and experience, I know BitcoinPostage.info to be a service which sells postage in exchange for Bitcoin. I further know that individuals involved in the distribution of narcotics on the darkweb in exchange for cryptocurrency utilize services like BitcoinPostage.info in order to avoid the currency exchange from Bitcoin to fiat currency and to conceal their illegal activities.

16. Additionally, a review of the return addresses found on the parcels received following purchases from Pill-Cosby and SlangGang show that these parcels consistently bear return addresses including the phrase "EBAY FULFILLMENT." Based on my training and experience, I know that individuals involved in the distribution of large quantities of drugs using the United States Postal Service often utilize fraudulent return addresses to appear consistent with legitimate businesses with a high volume of mailings, in order to hide their activity from law enforcement.

17. Specifically, on December 04, 2018, FDA-OCI agents acting in an undercover capacity placed an order for fifteen (15) pills advertised as "Pressed 30mg Oxy \$13 each." On December 11, 2018, investigators from the DEA and USPIS retrieved a parcel from the undercover address provided at the time of this purchase. The parcel contained fifteen (15) tablets, blue in color, round in shape, bearing the pill imprint "A 215" and a half tablet score. Additionally, the parcel containing the pills was found to bear postage purchased from EasyPost, and originated from the

Las Vegas, Nevada, area. A review of USPS databases indicates that these parcels were purchased by an EasyPost postage meter associated with BitcoinPostage.info. Subsequent analysis of these pills indicated that these pills did not contain oxycodone HCL but rather, contained fentanyl.

18. All of the parcels received following the purchase of pills from Pill-Cosby and SlangGang were found to contain pills packaged in a similar fashion and contained pills of similar shape, color, size, and bearing the pill imprint "A 215" and a half tablet score.

19. Records provided by Paypal, Inc., indicate that between on or about January 27, 2017 and on or about April 25, 2017, a Paypal account with ID #: ending in 4715 was used to send approximately \$3,800 (USD) in exchange for multiple items used in the manufacture of counterfeit drugs. Specifically, Paypal account ending in 4715 was used to purchase items with the following descriptions: "Handheld Manual Tablet Press Pill Maker TDP-00 making pills/tablet No die mould", "6mm A/215 Punching Die Mold Stamp for candy tablet press mold pill maker [TDP0/1.5]", "Automatic Electric Single Punch Tablet Press Pill Pellet Making Machine TDP-5", and "TDP-5 Tablet Press Machine 5000 Tablets/Hour Prompt Services Easy Maintenance."

20. Based on my training and experience, I know that it is common for individuals involved in the sale of counterfeit punches and dies to advertise them as having an intended use for the manufacture of candy or confections in order to conceal their activity from law enforcement. I also know that a TDP-5 tablet press, manufactured by LFA Machines Oxford LTD, is a 5 ton desktop tablet press capable of producing 5,000 tablets per hour.

21. A review of records related to Paypal account ending in 4715 show that the account was registered in the name KHLARI ISBELL SIROTKIN, social security number ending in -6210, Date of Birth (DOB) XX/XX/1983, the address 6260 REDWOOD LAS VEGAS, NV 89118, the

telephone numbers 702-91-1148¹ [sic] and (702) 569-9982, and the email address **KLIZOSIROTA@GMAIL.COM (SUBJECT GMAIL ACCOUNT 1)**.

22. Additionally, Paypal records indicate that Paypal account # ending in 3777 was registered in the name KHLARI SIROTKIN at the address 2735 W PEBBLE RD UNIT 313 LAS VEGAS, NV 89123, and the email address **KLIZOB@GMAIL.COM (SUBJECT GMAIL ACCOUNT 2)**.

23. Based on my training and experience, companies like Paypal communicate with their customers regarding records of transactions using the email address provided by the customer at the time of account registration.

24. I have viewed Nevada Department of Motor Vehicles (DMV) records including a photo of Khlari Sirotkin, with license number ending 2550, DOB XX/XX/1983, and address 2375 W. Pebble Rd. Unit 313, Las Vegas, NV 89123.

25. Records provided by Binance, Inc. indicate that on September 24, 2017, account # ending in 7827 was registered in the name Khlari Sirotkin with the email address ebank-mail@protonmail.com and the telephone number 702-901-1148. These records show that this account is responsible for receiving approximately 11.56 Bitcoin ("BTC"), which was equivalent to approximately \$59,000 (USD) using the exchange rate as of April 28, 2019.

26. Based on my training and experience, Binance, Inc. is a cryptocurrency exchange company that sells cryptocurrencies in exchange for fiat currencies.

27. Based on my training and experience, protonmail is an encrypted email service that utilizes end-to-end encryption to conceal the contents of email communication even from the

¹ At present, it is believed that this was a typo and that this number was intended to be the number indicated as 702-901-1148.

provider of the service. Based on my training and experience, I know that protonmail is also commonly used by individuals involved in drug trafficking on the darkweb in order to conceal their communication from law enforcement.

28. Records provided by BitPay, Inc. indicate that, on March 11, 2017 a cryptocurrency account was used to send funds to the merchant Anonabox, via the BitPay service. During this transaction, the purchaser provided the name Khlari Isabel Sirotkin, with the postal address as 2735 W Pebble Rd 313 LAS VEGAS, and the email address as **SUBJECT GMAIL ACCOUNT 1**.

29. A review of the Anonabox website indicates that they sell various computer networking equipment which incorporates the use of Virtual Private Networks (VPNs) and The Onion Router (TOR). A further review indicates that some of these products integrate the use of the "HideMyAss" VPN service.

30. Based on my training and experience, I know that TOR is an encrypted computer networking protocol developed by the U.S. Government to allow for anonymous encrypted communication. Furthermore, I know that the use of a TOR browser and the TOR protocol is the only way to access marketplaces such as Dream Market, Wall Street Market, and Empire Market. Furthermore, I know that VPNs are also commonly used by individuals involved in the distribution of narcotics on the darkweb, in order to conceal their access to TOR infrastructure from law enforcement.

31. A further review of records provided by BitPay, Inc. indicate that, on October 11, 2017, a cryptocurrency account was used to send funds to the merchant Ledger via the BitPay service. During this transaction, the purchaser provided the email address Ebank-mail@protonmail.com.

32. Based on my training and experience, I know Ledger to be a company that manufactures hardware devices specifically designed for the storage of cryptocurrency.

33. A review of records provided by Poloniex indicates that an account was created in the name Khlari Sirotkin, DOB: XX/XX/1983, address 2735 W Pebble Rd, Las Vegas, NV, email address crypto-banking@protonmail.com, and telephone #: 702-901-1148. Additionally, these records included a photo of an individual matching the description of Khlari Sirotkin holding a Nevada Driver License bearing the name Khlari Isabell Sirotkin, DOB XX/XX/1983, and license number ending in 2550. A further review of Poloniex records indicate that this account received approximately \$62,000 (USD) in various cryptocurrencies, including Bitcoin, between May 12, 2017 and August 30, 2017.

IP Address Analysis - 68.108.21.117

34. Records provided by Binance indicate that between November 29, 2017 and December 01, 2017, the Binance account created with the email address ebank-mail@protonmail.com was interacted-with by a computer assigned IP address 68.108.21.117 on two hundred and fifty-six (256) occasions.

35. Records provided by Coinbase indicate between December 12, 2017 and December 14, 2017, the Coinbase account created with email account **DJCADZOW@GMAIL.COM** (**SUBJECT GMAIL ACCOUNT 3**) was interacted-with on four (4) occasions by a computer assigned the IP address 68.108.21.117.

IP Address Analysis - 172.115.25.95

36. Records provided by Binance indicate that between December 22, 2017 and February 08, 2018, the Binance account created with the email address EBANK-

MAIL@PROTONMAIL.COM was interacted-with on fifty-eight (58) occasions by a computer assigned the IP address 172.115.25.95.

37. Records provided by Poloniex indicate between February 16, 2018 and March 21, 2018, the Poloniex account created with email account CRYPTO-BANKING@PROTONMAIL.COM was interacted-with on two (2) occasions by a computer assigned the IP address 172.115.25.95.

38. Records provided by BitPay indicate that on June 07, 2018, the BitPay account created with the email address **KELLYCOMATOSE@GMAIL.COM (SUBJECT GMAIL ACCOUNT 4)** was interacted-with by a computer assigned the IP address 172.115.25.95.

39. Records provided by BitPay indicate between June 11, 2018 and June 15, 2018, at 18:33 the BitPay account created with email account EBANK-MAIL@PROTONMAIL.COM was interacted-with by a computer assigned the IP address 172.115.25.95.

40. Records provided by BitPay indicate that on June 16, 2018 at 03:18, the BitPay account created with the **SUBJECT GMAIL ACCOUNT 4** was interacted-with on three (3) occasions by a computer assigned the IP address 172.115.25.95.

41. Records provided by BitPay indicate on June 16, 2018, at 05:20, the BitPay account created with email account EBANK-MAIL@PROTONMAIL.COM was interacted-with by a computer assigned the IP address 172.115.25.95.

42. Records provided by Coinbase indicate on August 13, 2018, the Coinbase account created with the **SUBJECT GMAIL ACCOUNT 3** was interacted-with on seven (7) occasions by a computer assigned the IP address 172.115.25.95.

IP Address Analysis – 73.98.45.214

43. Records provided by Coinbase indicate that between March 30, 2017 and June 22, 2017, the Coinbase account created with the **SUBJECT GMAIL ACCOUNT 3** was interacted-with on twenty-four (24) occasions by a computer assigned the IP address **73.98.45.214**.

44. Records provided by Poloniex indicate that between August 25, 2017 and August 27, 2017, the Poloniex account created with the email address **CRYPTO-BANKING@PROTONMAIL.COM** was interacted-with on four (4) occasions by a computer assigned the IP address **73.98.45.214**.

45. Records provided by Coinbase indicate that between October 12, 2017 and May 22, 2018 the Coinbase account created with the **SUBJECT GMAIL ACCOUNT 3** was interacted-with on seventy-one (71) occasions by a computer assigned the IP address **73.98.45.214**.

46. Records provided by Binance indicate that between July 09, 2018 and July 19, 2018, at 05:27, the Coinbase account created with the email address **CRYPTOKLIZO@GMAIL.COM** (**SUBJECT GMAIL ACCOUNT 5**) was interacted-with on sixty-seven (67) occasions by a computer assigned the IP address **73.98.45.214**.

47. Records provided by Binance indicate that between July 19, 2018, at 16:14 and 18:31, the Coinbase account created with the **SUBJECT GMAIL ACCOUNT 3** was interacted-with on two (2) occasions by a computer assigned IP address **73.98.45.214**.

48. Records provided by Binance indicate that between July 19, 2018 at 20:09 and October 10, 2018, the Coinbase account created with the **SUBJECT GMAIL ACCOUNT 5** was interacted-with on two hundred (200) occasions by a computer assigned the IP address **73.98.45.214**.

BACKGROUND CONCERNING EMAIL

49. In my training and experience, I have learned that Google LLC, provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google LLC, allows subscribers to obtain email accounts at the domain name for the **SUBJECT GMAIL ACCOUNTS**, such as the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google LLC. During the registration process, Google LLC, asks subscribers to provide basic personal information. Therefore, the computers of Google LLC, are likely to contain stored electronic communications (including retrieved and unretrieved email for Google LLC, subscribers) and information concerning subscribers and their use of Google LLC, services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

50. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

51. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can

include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

52. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

53. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy"

while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

54. Based on the foregoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

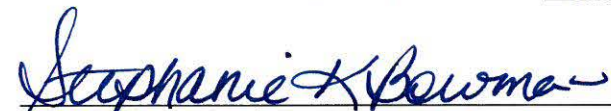
51. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully Submitted,



Paul W. Cox
Special Agent
Food and Drug Administration-Office of
Criminal Investigations

Subscribed and sworn to before me on the 1 day of ^{May}~~April~~ 2019



Honorable Stephanie K. Bowman
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with

KLIZOSIROTA@GMAIL.COM (SUBJECT GMAIL ACCOUNT 1)

KLIZOB@GMAIL.COM (SUBJECT GMAIL ACCOUNT 2)

DJCADZOW@GMAIL.COM (SUBJECT GMAIL ACCOUNT 3)

KELLYCOMATOSE@GMAIL.COM (SUBJECT GMAIL ACCOUNT 4)

CRYPTOKLIZO@GMAIL.COM (SUBJECT GMAIL ACCOUNT 5)

stored at premises owned, maintained, controlled, or operated by Google LLC, an email provided that is headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails, associated stored data, and cloud stored data associated with the account **January 1, 2017 to present**, including stored or preserved copies of files and emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1), 846, 331(a), 331(k), and 331(i), and Title 18, United States Code, Section 1957 (hereinafter the “TARGET OFFENSES”) involving Khlari Sirotkin, and occurring after **January, 01, 2017**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence indicating communication before and after the narcotics transactions.
- (b) Evidence indicating the transfer of narcotics between individuals.
- (c) Evidence indicating the cost and amount of narcotics transferred.
- (d) Evidence indicating transactions involving proceeds from drug sales
- (e) Evidence of the manufacture of counterfeit drugs
- (f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (g) Evidence indicating the email account owner’s state of mind as it relates to the crime under investigation;
- (h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).